# Mitigation Techniques of Blackhole Attack in DSR based MANET: An overview

[1]Vaishali B. Mewada, [2]Viral Borisagar

[1]ME scholar, [2]Associate Professor
Computer Science and Engineering Department
Government Engineering College, Sec-28, Gandhinagar, India
[1]vsl.239@gmail.com, [2]viralborisagar@yahoo.com

***Abstract*— Mobile ad Hoc Networks are Wireless, infrastructure less, Networks. Due to mobility and limited radio range, every node has to perform the dual responsibility of host of different services as well as routers for forwarding information. Different routing algorithms are used for transmitting the information such as DSDV, DSR, and AODV. These algorithms are designed earlier without taking care of security aspect, so transmitted information and network is vulnerable to different types of attacks. Most popular attack in MANET is Blackhole attack, which has the severe impact on network. In this paper, We will discuss the blackhole attack , its impact and different techniques of detecting and mitigate its effect on DSR based MANET.**

***Index Terms*—MANET, DSR, Black Hole**

## I. INTRODUCTION

Mobile Ad-hoc networks are composed of autonomous wireless nodes i.e. it requires no central node to manage the networks. All the work is done with the mutual agreement and understanding between the nodes. Thus every node will work in both configurations (Sometimes as router and sometimes as host) [1]. Because of mobility nature of nodes, topology of the network changes with time and makes the ad-hoc network to be a non–infrastructure network. Every node has the self configuring ability.

Because every node has to act as both host and router, Security problems are there in mobile ad hoc network. Every Node has the responsibility of forwarding the packets received by it. But due to lack of security mechanism in routing protocols, nodes can behave unexpectedly and absorbs the packets without forwarding it. There are various types of attacks that can occur in such a network, so it is essential to detect such kind of attack and methods to exclude the malicious or misbehaving nodes and enhance the nodes cooperation.

In this paper, Black hole attack, which is the famous denial of service attack, is discussed. In this attack, malicious node behave like a black hole and absorbs all the packets received by it. There should be mechanisms to detect and remove such nodes from the network for successful and errorless transmission of data. In this paper, various techniques to identify and removal of such black hole nodes are presented.

## II. SECURITY ATTACKS IN MANET

Attacks in MANET can be categorized into two parts: Active attacks and Passive Attack. A passive attack does not disturb the routing protocol operation, but only tries to find valuable information by listening to routing traffic, so it is very difficult to detect. An active attack is an effort to alter the data, authentication gain, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network. Active attack can be further divided into external attacks and internal attacks. An external attack is one in which participating nodes are not part of the network. An internal attack is one in which compromised or malicious node are part of the network. Internal attacks typically have more severe effect to the network, since malicious nodes are already part of the network as authorized parties. Therefore, such nodes should be protected with the network security mechanisms and underlying services [2].

Different types of Network Layer attacks are described below:

- BlackHole Attack: In this attack, malicious nodes absorb the packets received by it without forwarding to the next hop. It can either use the packet information for wrong purpose or discard the packets.
- Wormhole Attack: In this attack, a malicious node receives packets form one location in the network and tunnels them to another location in the network, where these packets are again sent into the network. This tunnel between two conspiring attackers is referred to as a wormhole [3].
- Byzantine Attack: A malicious intermediate node works alone, or a set of malicious intermediate nodes works in mutual agreement. Examples of such attacks are creating routing loops, forwarding packets using fake paths, or selectively dropping packets, which results in the degradation of the routing services and poor network performance [5].
- Sleep Deprivation Attack: This kind of Attack run out limited resources, like battery powers, in the mobile ad hoc nodes, by constantly making them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be caused by flooding the targeted node with unnecessary routing packets [4].
- Location Disclosure: In this attack, attacker reveals information regarding the location of nodes or structure of the network. It collects the various node location information and plans the further attacks.
- Eavesdropping: The purpose of this attack is to eavesdrop the secret information passing to the network. This Confidential information can be location of the nodes, passwords, public-private keys also.

- Flooding: In this attack, Networks are flooded by fake RREQ and data packets which create the congestion in the network and makes it difficult for the network to transmit the information to actual destination nodes.

In this paper, we focus on the black hole attack in DSR based network.

## III. DSR PROTOCOL

DSR protocol is the on-demand, reactive routing algorithm. It has two main mechanisms: Route discovery and Route Maintenance. When the source node wants to send data packets to destination and route is not stored on its cache then source node initiates routing discovery. Source node broadcasts Route Request packet (RREQ) to discover a route. RREQ packet contains destination address of the request Node, ID of this packet and route record. Here, the address of the request node and ID of this packet are used to identify the RREQ. When a node receives the RREQ packet forwarded by neighbor node, the node checks its cache. If the RREQ packet is there in recent received RREQ list, then discard it. If the address of this node is included in RREQ route record, discard this also. This is necessary to avoid the route looping. If the node is the destination node, then it delivers route reply packet (RREP). RREP contains the route (hop list) from source to destination nodes and it is sent to the source node via reverse path if the links are bidirectional or the destination node again initiate route discovery mechanism to find the route from destination node to source node. The sequence number in RREQ packet shows the freshness of the route record, so as to determine the next step only by comparing the sequence number when the node receives RREQ. So before forwarding the RREQ packet, the node will check up the route record in the packet. If the sequence number is higher, the node will write the route record into its cache. The advantage of this idea is to reduce the time of routing discovery of other nodes [6].

## IV. BLACKHOLE ATTACK AND DSR

Blackhole is a type of active internal attack, in which compromised nodes are part of the network itself and consumes the packets received to it without forwarding to next node. So the actual destination node cannot get the data packets intended to it. Figure shows the behavior of the network when the malicious nodes are present in the network.In black hole attack, a malicious node uses its routing protocol, DSR in this case, to advertise itself for having the shortest path to the destination node it wants to intercept. Black hole nodes can be identified by using two characteristics: first, node uses the ad hoc routing. Second, the node consumes the intercepted packets [8].

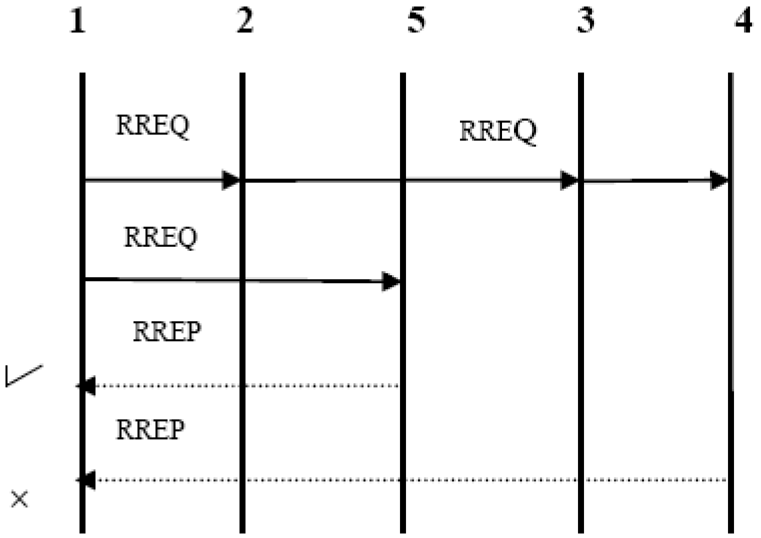

Fig. 1. MANET with malicious node

In Fig.1. simple mobile ad hoc network is presented, Here we assume that all the nodes, except 5 are genuine. Node 5 is the malicious node. Let us take node 1 as the source node and node 4 as the destination node.

Data Packets transmission using DSR protocol works as follows:

- Node 1 sends RREQ packet with id and destination address as parameters.
- Node 2 and Node 5 receives the RREQ packet.
- Node 2 forwards the packet to node 3, if it has no valid route to the destination node.
- Node 5, as it is the malicious node, doesn't check whether it has the route or not to the destination and send the RREP packet with the spurious route to source node 1.
- Source node considers this as valid route to node 4 and sends the data packets using the same route.
- Node 5 consumes or discards the packets received to it without forwarding to next node.

So, the data transmission will not be successful. Therefore, there must be ways to identify such malicious nodes and prevent them for taking part in routing procedure.

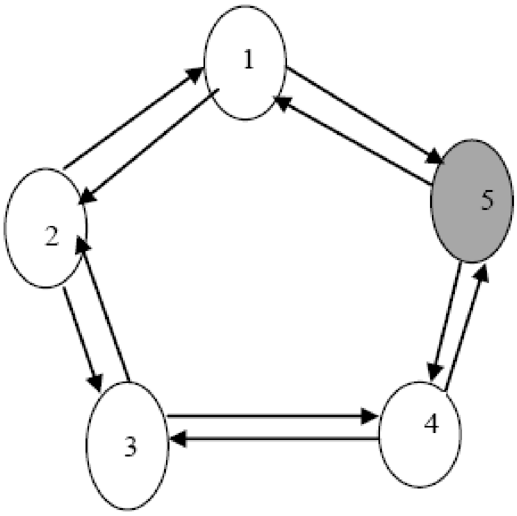

Fig. 2. Route Discovery in presence of malicious node

## V. Black Hole detection and Mitigation Techniques review

There are many methods proposed in the literature to detect, prevent and reduce the effect of blackhole node attack. Some of them are discussed below:

In paper [6] authors proposed a scheme, SRSN, based on the sequence number and end-to-end acknowledgement method to check the strictly increment of the sequence number of RREQ. Three data structure is maintained: Trusted Routing List, Suspicious Routing List and RREQ_ACK_REQ list. The scheme works as follows: If the destination has trusted record about the source, it will check the sequence number difference of RREQ. If it is 1, then route record is valid, or the route record is in status of suspicious. If the destination has not any record about the source, then it is considered as suspicious. In both the cases, end to end acknowledgement is used to validate the suspicious route. If is validated, then it will be moved to the trusted route record. This method does little edition to DSR algorithm. Discontinuity of sequence number of the received packets helps to identify the malicious nodes.

- In paper [9], author adopted biological example, proposed by Dawkins, to calculate the association between the nodes which can be Companion, Known or Unknown. Trust estimator equation and threshold values are calculated and based on them, most trusted path, giving the priority to companion is selected.
- In paper [10], author proposed a BDSR scheme, the proactive and reactive defense architecture. Authors presented an algorithm which has two functions: First is, initiate, which identifies the blackhole nodes by sending bait RREQ using virtual and nonexistent destination address to bait the malicious nodes to reply to RREP. If any node responds to this request, it will be identified as malicious node and added in the blackhole list. Then second function start is called which performs the normal DSR route discovery. During this Start function, if the packet delivery ratio gets lower than the threshold value, then the again initiate function is called to identify the malicious nodes or the route discovery will be considered as successful and data packets transmission takes place.
- The method in [11] is the extension of BDSR scheme. In BDSR, It is not specified that how to select virtual destination address to bait the malicious nodes. In CBDS, virtual destination address for the bait RREQ is selected as one hop neighbor from the source. If any node other than this neighbor replies to RREQ then it is certain that malicious nodes are present in that path. The node which replies to the RREQ is considered as black hole node also. Then reverse tracing method is used to identify the malicious nodes.
- In paper [1], two solutions are proposed to battle against blackhole attack. First is to find the redundant paths with the shared nodes. It is the secure but the delay is higher. Second method is to check the sequence number of packets sent and received. It is not that much secure but highly efficient method.
- In [12], authors proposed a method to find the secured path based on human trust analogy. For finding the route from source to destination, path's trust value is computed for the most secured path. Trust value is equal to the minimal one of the nodes' value in the path. In this method, nodes derive their trust factors from experience, knowledge and recommendation from other nodes. Linear aggression method is used to estimate the overall trust in a node and a minimal value is used to compute a path's trust.
- In the DBA-DSR scheme in [13], Authors use the fake RREQ packets to identify the malicious nodes in the network before the actual routing takes place. This scheme also uses the acknowledgement mechanism by source and intermediate nodes, if the fake RREQ –RREP fails to identify the node black hole nodes. There are two drawbacks of this scheme. First is, as the acknowledgement packets are exchanged to check whether the intermediate node is fake or not, routing overhead increases with this scheme. Second drawback is the longer time needed to find the routes if the distance between the source and intermediate is long.

- The scheme proposed in paper [14] removes the disadvantages of the DBA-DSR algorithm and presents a modified way to detect the blackhole nodes using the acknowledgement packets sent by the previous node of the intermediate node. Using this approach blackhole node list is updated and routing overhead and route discovery period decreases.
- Authors uses the source routing and caching property of DSR to prevent the blackhole attack in the network in paper [15]. After the detection of blackhole node or misbehaving node, blackhole node id is passed to addtopath function of DSR based on priority. All the paths are parsed and if the blackhole node appears in path then dump that path and add all rest of paths for the source to particular destination. This method uses the normal cache processing time and packet drop ratio is also reduced.

## VI. CONCLUSION

Security is an important factor in mobile ad hoc networks as routing protocols have not any security aspect in built. Various types of attacks are possible on MANET, one of them is blackhole. Network throughput and performance of the network degrades because of such attacks. Various techniques are discussed in this paper and there is a lot more scope to optimize the techniques to make network more efficient and secure.

## REFERENCES

[1] Ms.Nidhi Sharma Mr.Alok Sharma “Blackhole node attack in MANET,” 2012 Second International Conference on Advanced Computing & Communication Technologies.

[2] J. Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing security in wireless ad Hoc networks”, IEEE Communication Magazine, October 2002.

[3] Abhay Kumar Rai, Rajiv Ranjan , Saurabh Kant, “Different types of attacks on integrated MANET-Internet communication,” International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).

[4] Himadri Nath Saha, Dr. Debika Bhattacharyya,Dr. P. K.Banerjee, Aniruddha Bhattacharyya ,Arnab Banerjee, Dipayan Bose, “Study Of different attacks in MANET with its detection & mitigation scheme”, International Journal of Advanced Engineering Technology, E-ISSN 0976-3945, IJAET/Vol.III/ Issue I/January-March, 2012/383-388

[5] Praveen lalwani, Dr. Sanjay Silakari, Piyush Ku Shukla,” Optimized and executive survey on mobile ad-hoc network”, 2012 International Symposium on Cloud and Services Computing, 978-0-7695-4931-6/12, 2012 IEEE DOI 10.1109/ISCOS.2012.37

[6] Jieying Zhou, Junwei Chen, Huiping Hu,” SRSN: Secure routing based on sequence number for MANETs”, 1-4244-1312-5/07/ 2007 IEEE

[7] Swati Jain1, Naveen Hemrajani2,” Detection and mitigation techniques of black hole attack in MANET: An Overview”, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[8] Ashish T. Bhole, Prachee N. Patil, “Study of blackhole attack in MANET”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012

[9] N.Bhalaji, Dr.A.Shanmugam,” Association between nodes to combat blackhole attack in DSR based MANET”, 978-1-4244-3474-9/09, IEEE 2009

[10] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han- Chieh CHAO, Jiann-Liang CHEN, “Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs”, ICACT, February 2011

[11] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, “CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture”, 978-1-4577-0787-2/11, 2011 IEEE

[12] Yogendra Kumar Jain, NIkesh Kumar Sharma,“ Secure trust based dynamic source routing in MANETs”, International Journal of Scientific and Engineering Research Volume 3, Issue 8, August 2012.

[13] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, Mohammad S. Obaidat, “Detecting blackhole attacks on DSR- based mobile ad hoc networks”, 978-1-4673-1550- 0/12, IEEE 2012

[14] Chandar Diwaker, Sunita Choudhary, “ Detection of blackhole attack In DSR based MANET”, International Journal of Software and Web Sciences, 2013

[15] Prachee N. Patil, Ashish T. Bhole, “ Black hole attack prevention in mobile ad hoc networks using route caching”, 978-1-4673-5999-3/13, IEEE 2013